Chancen und Risiken LDAP-basierter zentraler Authentifizierungssysteme

11. DFN-CERT/PCA Workshop
„Sicherheit in vernetzten Systemen“
4. Februar, Hamburg

Peter Gietz, CEO, DAASI International GmbH
Peter.gietz@daasi.de

DAASI International
Directory Applications for Advanced Security and Information Management

Agenda

- Identity Management
- Kurzdarstellung von LDAP
- Authentifizierung in LDAP
- LDAP für Authentifizierung bei Login-Prozessen
- Authentifizierung und Autorisierung in Anwendungen
- Integrationsmöglichkeiten

DAASI International
Directory Applications for Advanced Security and Information Management

DFN Projekte als Ursprung von DAASI International

- Seit 1994 vom BMBF finanzierte DFN-Forschungsprojekte zu Verzeichnisdiensten an der Universität Tübingen
- Wegen Aufbau und Betrieb von Diensten, die nicht durch Forschungsmittel Förderungsfähig sind musste neue Organisationsform gefunden werden
- Januar 2001 wurde deshalb die DAASI International GmbH gegründet
- Das letzte DFN-Verzeichnisdienst-Projekt wurde von DAASI International durchgeführt
  - Ein Teil der hier vorgestellten Ergebnisse stammen aus diesem Projekt

DAASI International
Directory Applications for Advanced Security and Information Management

Identity Management

DAASI International
Directory Applications for Advanced Security and Information Management

Identität in Identity Management

- Eindeutige Kennung, die eine Person gegenüber einem Computersystem identifiziert
  - Z.B. Login-Id, einen Zusammenhang mit einer Person bedeutet
- Eine Person kann in verschiedenen Zusammenhängen verschiedene Identitäten haben
  - Unterschiedliche Computersysteme
  - Unterschiedliche Rollen bei einem Computersystem
- Auch andere Entitäten als Personen können in diesem Sinn Identitäten sein, z.B. Computerprogramme, Computer, etc.

DAASI International
Directory Applications for Advanced Security and Information Management

Was soll Identity Management?

- Personen wollen:
  - Informationen über sich veröffentlichen, um z.B.kontaktiert werden zu können
  - Informationen über andere Personen erhalten
  - Sich authentifizieren, also ihre Identität beweisen, um Ressourcen und Dienste in Anspruch nehmen zu können
  - Im Netz bezahlen
- Organisationen wollen
  - Identitätsinformationen über Mitarbeiter oder Mitglieder verwalten
  - Benutzer ihrer Ressourcen verwalten
  - Konsistenz der Identitäten in verschiedenen Informationsspeicher erreichen
  - Vortäuschung falscher Identitäten verhindern
- Mobilität erhöht die Anforderungen an Identity Management

DAASI International
Directory Applications for Advanced Security and Information Management

Prozesse

- Personen
  - Werden in Organisationen aufgenommen
  - Erhalten Rollen und Berechtigungen
  - Agieren in ihrer Rolle
  - Wechseln Rollen und Berechtigungen
  - Verlassen die Organisation
- Organisationen bzw. Organisationseinheiten
  - Werden gegründet
  - Agieren in Arbeitsprozessen
  - Werden zusammengefügt (merge)
  - Werden aufgeteilt (split)
  - Werden aufgelöst

DAASI International
Directory Applications for Advanced Security and Information Management

Abbildung der Prozesse im Identity Management

- Identitäten: erzeugen
- Identitätsinformationen aktualisieren
- Identitäten löschen
- Identitäten archivieren
- Identitätsinformation anfordern und anzeigen
- Identitäten verifizieren
- Mit Identitäten signieren (PKI)
- Zugriffskontrollregeln durchsetzen (lese und schreibrechte)
- Datenbanken für Identitäten aufbauen und pflegen
- Identitätsdatenbanken synchronisieren
- Identitätsdatenbanken aufteilen und zusammenführen

Nach: The Open Group: Business Scenario: Identity Management, 15. July 2002, www.opengroup.org

DAASI International
Directory Applications for Advanced Security and Information Management

Was gehört zu Identity Management?

- Passwort-Verwaltung und –Synchronisierung
- Identitätszertifizierung mit Public Key Infrastructure
- Externe Identitätsdienste (MS Passport, Liberty Alliance)
- Single Sign On Mechanismen
- Rollenkonzepte und Berechtigungen
- Verwaltung des Zugriffs auf Ressourcen
- Authentifizierung und Autorisierung
- Verzeichnisdienste kann genutzt werden zur Speicherung von Identitätsinformation, Passwörtern, Zertifikaten, Rollen und Berechtigungen, Policy
- Metadirectories dienen zur Synchronisierung verschiedener Datenspeicher und Vermeidung von Inkonsistenzen
- Provisioning Systeme verwalten Berechtigungen und versorgen Anwendungen mit Identitätsinformation

DAASI International
Directory Applications for Advanced Security and Information Management

Kurzdarstellung von LDAP

DAASI International
Directory Applications for Advanced Security and Information Management

Was ist LDAP

- Lightweight Directory Access Protocol
- Ein Datenbankmodell (X.500)
  - Hierarchische Datenstruktur
  - Objektorientierter Ansatz
  - Erweiterbar für beliebige Daten
- Ein Netzwerkprotokoll
  - Internetstandard
  - Flexibel erweiterbar
  - Verteilung der Daten im Netz
  - Spiegelung der Daten im Netz

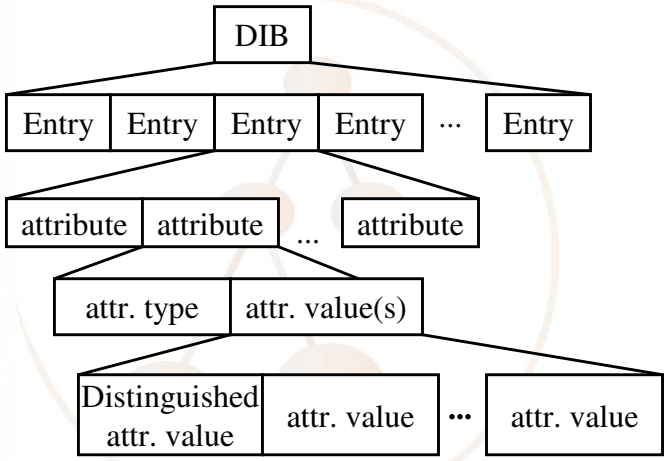
DAASI International
Directory Applications for Advanced Security and Information Management

LDAP Informationsmodell

- Ein Datensatz wird Eintrag (entry) genannt
- Ein Eintrag besteht aus Attributen
- Ein Attribut besteht aus Attributtyp und Attributwert
- Attributtyp Definition kann u.a. enthalten:
  - Attributsyntax
  - Single- oder Multivalued
  - verschiedene Vergleichsregeln (Matching Rules)
    - *Equality*, *Substring*, *Ordering*, *Extensible* (selbstdefiniert)
- Ein oder mehrere Attributtyp-Wert-Paare bilden den Namen des Eintrags
- Jeder Eintrag hat mindestens ein *Objektklassen-Attribut* haben
  - Charakterisiert den gesamten Eintrag
  - Spezifiziert zu verwendende Attributtypen (*MUST und MAY*)
  - Objektklassen können Eigenschaften von übergeordneten Objektklassen ererben

DAASI International
Directory Applications for Advanced Security and Information Management

Directory Information Base



DAASI International
Directory Applications for Advanced Security and Information Management

Beispiel

DN: cn=Mister X, o=University, c=NL

ABSTRACT →	**objectClass=top**
STRUCTURAL (nur eine Vererbungshierarchie) →	**objectClass=person** **objectClass=organizationalPerson** **objectClass=inetOrgPerson**
AUXILIARY →	**objectClass=pKIUser**
cn aus person →	**cn=Mister X** **cn=Xavier Xerxes**
mail aus inetOrgperson →	**mail=X@dot.com** **mail=Mister.X@dot.com**
telephoneNumber aus organizationalPerson →	**telephoneNumber=1234567**
userCertificate aus pKIUser →	**userCertificate=a1b2c3d4e5f6…**

DAASI International
Directory Applications for Advanced Security and Information Management

Offene Struktur

- Mann kann eigenes Schema definieren
  - Objektklassen
  - Attribute
  - [Syntaxen]
  - [Matching Rules]
- Lokal kann man selbstdefiniertes Schema einfach verwenden
- Wenn das Schema global genutzt werden soll muss man es
  - Standardisieren (IETF-RFC)
  - Oder wenigstens registrieren (schemareg.org)

DAASI International
Directory Applications for Advanced Security and Information Management

Directory Information Tree (DIT)

- Daten werden in Einträgen gespeichert
- Einträge werden als Baumknoten gespeichert
  - Jeder Knoten hat 0 bis n Kinderknoten
  - Jeder Knoten hat genau 1 Elternknoten
    - Mit Ausnahme des Wurzelknotens
- Jeder Knoten hat einen eindeutigen Namen
  - In der eigenen Hierarchieebene: Relative Distinguished Name (RDN)
  - Alle RDNs auf dem Pfad von der Wurzel zum Eintrag bilden zusammen den Distinguished Name (DN)
  - Keine zwei Geschwistereinträge (also mit gemeinsamen Elternknoten) dürfen den gleichen RDN haben
  - Demnach hat kein Eintrag im gesamten Baum einen gleichen Namen

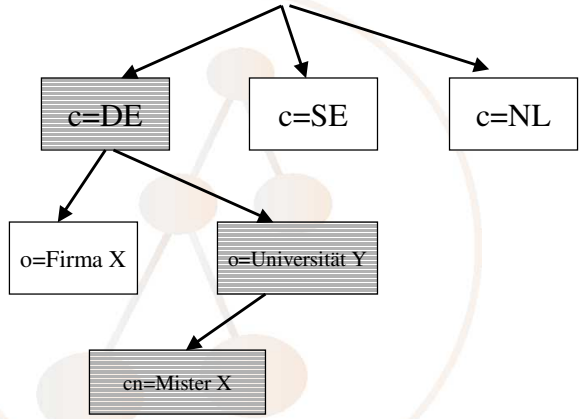
DAASI International
Directory Applications for Advanced Security and Information Management

DIT, RDN, DN

RDN: c=DE
(countryName)

RDN: o=Universität Y
(organizationName)

RDN: cn=Mister X
(commonName)



DN: cn=Mister X, o=Universität Y, c=DE

DAASI International
Directory Applications for Advanced Security and Information Management

Funktionsmodell

- Authentifizierungs-Operationen (s.u.):
  - bind
  - unbind
  - abandon
- Abfrage-Operationen:
  - search
  - compare
- Update-Operationen:
  - add
  - delete
  - modify
  - modifyDN

DAASI International
Directory Applications for Advanced Security and Information Management

Was gehört noch zum LDAP Standard?

- Neben dem Informationsmodell und dem Operationsmodell gehören zum LDAP-Standard u.a.:
  - LDIF, LDAP Data Interchange Format, [RFC 2849] ein ASCII-Format, mittels dessen man LDAP-Daten bequem austauschen kann.
  - LDAP URL [RFC 2255], ein URL-Format, welches die gesamte reiche Funktionalität der Search-Operation abbildet.
  - de facto sogar eine Bibliothek für C und Java, da alle Hersteller von SDKs die beiden entsprechenden Internet-Drafts implementiert haben.

DAASI International
Directory Applications for Advanced Security and Information Management

Authentifizierung in LDAP

DAASI International
Directory Applications for Advanced Security and Information Management

Authentifizierung

- Simple Bind
  - Man authentifiziert sich über einen Eintrag mittels DN und Passwort
  - Passwort geht ungeschützt über das Netz!
- Simple Bind + TLS (Transport Layer Security ~= SSL)
  - TLS verschlüsselt die gesamte Client Server-Kommunikation, sodass auch das Passwort beim Bind-Vorgang nicht als Klartext über das Netz geht
  - StartTLS-Operation
- Alternative Authentifizierung mittels SASL
  - Simple Authentication and Security Layer
  - beliebige SASL-Mechanismen verwendbar
  - Wenn von Client und Server unterstützt

DAASI International
Directory Applications for Advanced Security and Information Management

SASL Mechanismen 1/2

- PLAIN
  - einfacher Passwortmechanismus
  - nicht besser ist als simple bind ☹
- KERBEROS_V4
  - Kerberos Version 4 wegen Sicherheitsmängel obsolet ☹
  - ermöglicht Single Sign On (SSO) = einmaliger Authentifizierungsprozess gültig für verschiedene Anwendungen
- GSSAPI
  - Generic Security Service Application Program Interface, v2: RFC 2078
  - gekapselte Schnittstelle die weitere Authentifizierungsmechanismen integriert
  - Die beiden wichtigsten GSSAPI-Mechanismen sind:
    - Kerberos V5 ([RFC 1510]) ohne Sicherheitsmängel ☺
    - X.509 [X.509] basierte sogenannte strong authentication, bei der die Authentifizierung über Clientzertifikate geschieht (=x500 storng bind)

DAASI International
Directory Applications for Advanced Security and Information Management

SASL Mechanismen 2/2

- DIGEST MD5
  - Challenge-Response-Verfahren RFC 2831
  - Beruht auf MD5-Hash-Algorithmus [RFC 1321]
  - Server schickt einen Zufallstext an den Client; dieser errechnet einen auf diesem Text und das Passwort basierenden Hash, den er an den Server zurückschickt. Dieser berechnet ebenfalls den Hash und kann dadurch feststellen, ob der Client im Besitz des richtigen Passwortes ist, ohne dass dieses über das Netz geschickt werden musste.
- EXTERNAL
  - Verwendet eine bereits auf unteren Protokollschichten etablierte Authentifizierung für die Anwendungsschicht, z.B.:
    - X.509 auf der Transportschicht mittels IPSec [RFC 2401]
    - oder auf der Session-Schicht mittels SSL/TLS [RFC 2246]

DAASI International
Directory Applications for Advanced Security and Information Management

Welche Mechanismen sind Pflicht?

- RFC 2829 spezifiziert, welche Authentifikations-mechanismen in LDAP unterstützt werden müssen:
  - anonyme Authentifizierung (keine Authentifizierung, oder simple bind mit leerem Passwort)
  - Passwortauthentifizierung mittels des SASL-Mechanismus DIGEST MD5
  - durch TLS geschützte Passwortauthentifizierung mittels simple bind oder TLS geschützte Authentifizierung mittels des SASL-Mechanismus EXTERNAL
- Es wird aber in der Regel mehr implementiert
- Server zeigt an, was er unterstützt

DAASI International
Directory Applications for Advanced Security and Information Management

LDAP für Authentifizierung bei Login-Prozessen

DAASI International
Directory Applications for Advanced Security and Information Management

Ausgangslage: LDAP basierte Kontaktdateninformationsdienste

- Die klassische Anwendung (ITU)
- Entsprechendes Schema bereits im Standard definiert
  - Personendaten (White Pages)
  - Organisationsdaten (Yellow Pages)
- Organisationsstruktur abbildbar
- Elektronisches Telefonbuch
- Elektronisches Emailverzeichnis
- Grundlage für viele weitere Anwendungen, z.B: elektronisches Vorlesungsverzeichnis

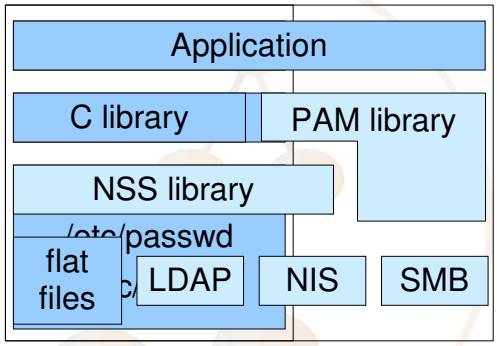
DAASI International
Directory Applications for Advanced Security and Information Management

Unix-Benutzerverwaltung

- Standardisierte LDAP Objektklassen zur Abbildung von NIS (RFC 2307), z.B.:
  - UNIX user (/etc/passwd and shadow file)
  - Groups (/etc/groups)
  - IP services (/etc/services)
  - IP protocols (/etc/protocols)
  - IP hosts and networks
  - MAC addresses
  - Boot information
- Kann über Name Service Switch (NSS) angesprochen werden (NSS-LDAP)

DAASI International
Directory Applications for Advanced Security and Information Management

Unix Authentifizierung



DAASI International
Directory Applications for Advanced Security and Information Management

Authentifizierungsdienst

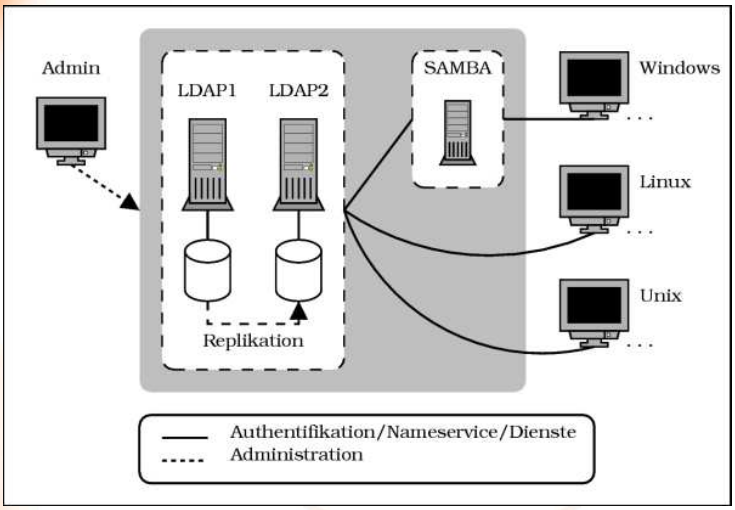
- Problem:
  - Benutzer haben Zugriff auf viele Rechner
  - Auf jedem Rechner eigene LoginID und Passwort
  - Benutzer muss sich viele Passwörter merken
  - Unterschiedliche Password-Policies
  - ➔ sehr hoher Administrationsaufwand
- Lösung:
  - Unified Login durch zentralen verzeichnisdienst-basierten Authentifizierungsdienst

DAASI International
Directory Applications for Advanced Security and Information Management

Zentraler verzeichnisdienstbasierter Authentifizierungsdienst

- Unix-Clients
  - Können mittels NSS / PAM-LDAP direkt auf LDAP-Server zugreifen
  - Kann gecashed werden: nscd (Name Service Caching Daemon)
  - Aber auch Anbindung an MS Active Directory (AD) möglich mit Kerberos
- Windows-Clients
  - Einfache Integration in AD
  - Aber auch über SAMBA Anbindung an LDAP-Server möglich
    - NT4 Domäne (Samba 2.x)
    - AD-Simulation (Samba 3.0)

DAASI International
Directory Applications for Advanced Security and Information Management



DAASI International
Directory Applications for Advanced Security and Information Management

Login-Lösung funktioniert z.B. mit

- Unix:
  - Linux
  - FreeBSD
  - OpenBSD
  - NetBSD
  - Solaris
  - HP-UX
  - AIX
- Windows:
  - 2000
  - XP

DAASI International
Directory Applications for Advanced Security and Information Management

Unified Login und Single Sign On (SSO)

- Mit dem Authentifizierungsdienst lässt sich nicht nur das Login realisieren
- Er lässt sich auch in verschiedene Netzanwendungen integrieren, z.B.:
  - IMAP, POP, SMTP auth, FTP, SSH, ...
- Viele Produkte bereits „LDAP-Enabeled“
- Wo noch nicht vorhanden, lassen sich LDAP-Schnittstellen einbauen (Voraussetzung: Open Source)
- Mit Kerberos lässt sich Single Sign On (SSO) erreichen:
  - Einmalige Passworteingabe und beliebige Ressourcennutzung für eine bestimmte Zeitspanne

DAASI International
Directory Applications for Advanced Security and Information Management

Zusammenfassung Authentifizierungsdienst

- Vorteil: Ein Passwort für alle Rechner
  - Der User muss sich weniger merken
  - Der Administrator und Help Desk wird erheblich entlastet
  - Passwortqualität zentral kontrollierbar
  - Vereinheitlichung der Authentifizierungsschnittstellen
  - Zwingt zu einem Gesamtkonzept
- Nachteil: Ein Passwort für alle Rechner
  - Single point of failure
  - Größerer Schaden bei Kompromittierung

DAASI International
Directory Applications for Advanced Security and Information Management

Passwörter in LDAP

- Standard Attribut userPassword
- Passwortspeicherung im Server:
  - Klartext ☹
  - Verschlüsselt (crypt, md5 und sha, smd5 ssha) ☺
- RFC 3062 spezifiziert Erweiterung des LDAP-Protokolls
  - Server verarbeitet und speichert das vom geschickte neue Passwort entsprechend seiner Konfiguration
  - Client muss diese nicht kennen
- RFC 3112 spezifiziert das neues Attribut authPassword
  - eigene Syntax für verschlüsselte Passwörter

DAASI International
Directory Applications for Advanced Security and Information Management

Sicherheitsrisiken

- Single point of attack
- Es gibt dedizierte LDAP Hacker-Tools
  - Kold „Knocking on LDAPs Door“ (www.phenoelit.de) online dictionary attack
  - Lumberjack (ebenfalls www.phenolit.de) brute force attack auf LDIF-Dateien
- "Man in the Middle Attack" und das Abhören von Netzverbindungen wie bei allen Netzprotokollen

DAASI International
Directory Applications for Advanced Security and Information Management

Gegenmaßnahmen

- Root-Passwörter sollten nicht in das zentrale System integriert werden!
- Netzkommunikation mit TLS verschlüsseln
  - Am besten mit Clientauthentifizierung
- LDIF-Dateien
  - verschlüsseln, wenn sie über das Netz verschickt werden
  - auch auf der Festplatte schützen!
- Password Policy definieren und erzwingen
  - In OpenLDAP noch nicht implementiert
  - Kann als Clientanwendungen implementiert werden

DAASI International
Directory Applications for Advanced Security and Information Management

Authentifizierung und Autorisierung in Anwendungen

DAASI International
Directory Applications for Advanced Security and Information Management

Generischer Prozess für Authentifizierung in Anwendungen

1. [Anwendung authentifiziert sich selbst einmalig mit einer Bind-Operation an einem dedizierten LDAP-Eintrag]
2. Anwendung erfragt vom Benutzer eine LoginId (anstelle eines LDAP-DNs) und Passwort.
3. Anwendung sucht anhand der LoginID den relevanten LDAP-Eintrag suchen.
4. Anwendung führt Bind-Operation an ermittelten Eintrag mit dem vom Benutzer mitgegebenen Passwort durch. Nach dem Erfolg dieser Bind-Operation kann der Benutzer als authentifiziert gelten.
5. [Anwendung beendet die Session mit unbind]
6. [Nach Beendigung aller Abfragen kann sich die Anwendung mit einem unbind abmelden]

DAASI International
Directory Applications for Advanced Security and Information Management

Beispiel Apache: Konfigparameter für LDAP Authentifizierung

- AuthLDAPURL
  - LDAP-URL mit LDAP-Servernamen und -Port sowie BaseDN und Suchtiefe ("sub" für den gesamten Teilbaum, "one" für nur eine Hierarchieebene unter dem BaseDN)
  - An der Stelle der URL, an der normalerweise die zurückzugebenden Attribute angegeben werden, das LDAP-Attribut, in dem der vom Benutzer angegebene Username/LoginId gesucht werden soll
  - [LDAP-Filter, der mit dem automatisch von mod_auth_ldap gebildeten Filter „ (<attr=username>)“ mit logischem UND kombiniert wird.
- AuthLDAPBindDN
  - optionaler DN, an dem sich mod_auth_ldap vor der Such-Operation authentifizieren kann.
- AuthLDAPBindPassword
  - das zu diesem BindDN gehörige Passwort.

DAASI International
Directory Applications for Advanced Security and Information Management

Beispiel Apache: Konfigparameter für LDAP Autorisierung

- Erweiterung des Parameters require:
  - require valid-user: Zugriff für alle, die sich erfolgreich am LDAP-Server authentifiziert hat.
  - require user <Benutzername>: Jeder einzelne berechtigte Benutzer wird angegeben
  - require dn: Einzelne Benutzer bezeichnet mit ihrem DN, anstelle des Werts des Attributs <attr>
  - require group <Gruppenname>: Zugriff für alle, die in einer mit einem DN bezeichneten Gruppe Mitglied sind
    - **AuthLDAPGroupAttributeIsDN on|off:**
      - DN des Gruppenmitglieds oder
      - der durch das Attribut <attr> bezeichnete Benutzer in den Werten der Attribute member und uniquemember gesucht.
    - **AuthLDAPGroupAttribute: Hiermit kann man andere Attribute als member oder uniquemember angeben, in denen dann anstelle dieser nach Gruppenmitgliedern gesucht wird.**

DAASI International
Directory Applications for Advanced Security and Information Management

Integrationsmöglichkeiten

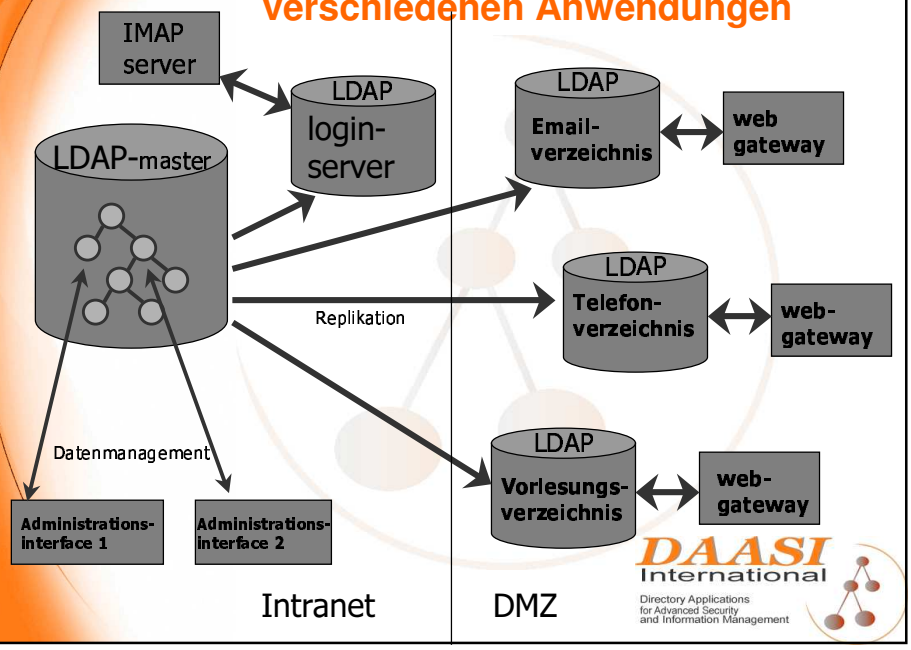
DAASI International
Directory Applications for Advanced Security and Information Management

Erweiterbarkeit von Verzeichnisdiensten

- Gleiche Daten - Verschiedene Dienste
  - Z.B.: Eine Datenstruktur, beliebig verteilt und/oder (teil)repliziert für:
    - Emailverzeichnis
    - elektronisches Telefonbuch
    - Benutzerverwaltung und Authentifizierungsdienst
    - Elektronisches Vorlesungsverzeichnis
  - Einfach weitere Objektklassenattribute zum Eintrag hinzufügen und neues Benutzerinterface (z.B. über das WWW) implementieren
  - Dies führt zu erheblichen Kosteneinsparungen

DAASI International
Directory Applications for Advanced Security and Information Management

Beispiel für zentrales Verzeichnis mit verschiedenen Anwendungen



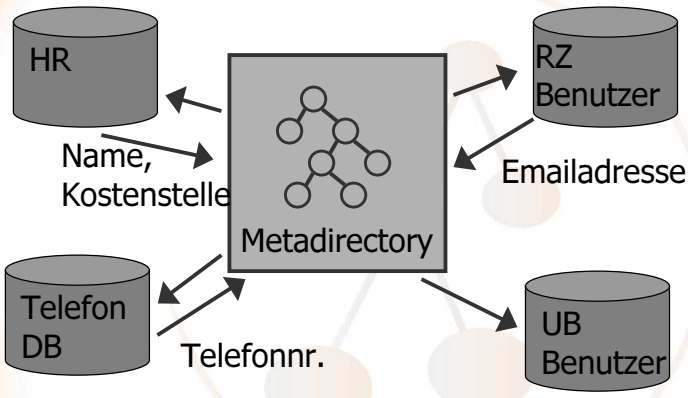
DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory

- Verknüpfung verschiedener Datenbanken, die verwandte Daten enthalten, z.B.:
  - Emailbenutzerdatenbank
  - Personaldatenbank
  - Telefondatenbank
- Die gleichen Daten müssen nur einmal eingegeben, bzw. gepflegt werden
- In den verknüpften Datenbanken werden sie automatisch angelegt bzw. geändert
- Eine übergreifende Sicht auf alle Daten
- Prozesse sind flexibel an Organisationsabläufe anpassbar

DAASI International
Directory Applications for Advanced Security and Information Management

Metadirectory Beispiel einer Universität



DAASI International
Directory Applications for Advanced Security and Information Management

Vielen Dank für Ihre Aufmerksamkeit!

- DAASI International GmbH
  - http://www.daasi.de
  - Info@daasi.de
- DFN Directory Services
  - http://www.directory.dfn.de
  - Info@directory.dfn.de

DAASI International
Directory Applications for Advanced Security and Information Management